UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/808,341	03/14/2001	James Riordan	CH920000012US1	3840

7590 09/13/2004

Louis P. Herzberg
IBM Corporation
Intellectual Property Law Dept.
P.O. Box 218
Yorktown Heights, NY 10598

EXAMINER	
AKPATI, ODAICHE T	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 09/13/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/808,341	RIORDAN, JAMES	
	Examiner	Art Unit	
	Tracey Akpati	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-15 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-15 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 14 March 2001 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 005.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-4, 11-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Curtis (6023764).

With respect to Claim 1, the limitation of "receiving from said message-originator program (D) a message comprising a program-specific identifier *(H(D))*, which has been provided for said message-originator program (D) by means of a trusted computing base (TCB)" is met on column 3, lines 34-39, column 6, lines 34-38, 44-49, 64-67; and "verifying whether said received program-specific identifier *(H(D))* is known to said message-receiver program (S)" is met on column 6, line 67 and on column 7, lines 1-2. The Java applet web server certificate represents the message receiver originator. The database or list of approved certificates represents the TCB. The certificate represents the program specific id because it performs the role of an identifier to the server.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the Java applet web server represent the message receiver originator because message requests originates here before the request is sent to the web server. The Java applet is located at the client.

With respect to Claim 2, the limitation of "sending from said message-originator program (D) to said message-receiver program (S) a message comprising a program-specific identifier *(H(D))*, which has been provided for said message-originator program (D) by means of a trusted computing base (TCB), said program-specific identifier (H(D)) being verifiable at said message-receiver program (S) whether it is known to said message-receiver program (S)" is met on column 6, lines 64-67 and on column 7, lines 1-2.

With respect to Claim 3, the limitation of "providing a program-specific identifier *(H(D))* for said message-originator program (D) by means of a trusted computing base (TCB) sending from said message-originator program (D) to said message-receiver program (S) a message comprising said program-specific identifier (H(D))" is met on column 6, lines 64-67; and "receiving at said message-receiver program (S) said message; and verifying whether said received program-specific identifier (H(D)) is known to said message-receiver program (S)" is met on column 6, line 67 and on column 7, lines 1-2.

With respect to Claim 4, the limitation of "a response-program-specific identifier (H(S)), which has been provided for said response-message-originator program by means of the trusted computing base (TCB) and an acknowledgment if the program-specific identifier *(H(D))* has been verified as being known" is met on column 7, lines 2-4. The client's sending of its certificate to the server serves as an acknowledgement that the program specific identifier H(D) of the server i.e. the server's certificate has been verified by the client.

With respect to Claim 11, the limitation of "wherein the message-originator program (D) and the message-receiver program (S) are executed on different systems and are connectable via a network, each having its trusted computing base (TCB) for providing program-specific cryptographic identifiers" is met on column 3, lines 45-52.

With respect to Claim 12, the limitation of "program code means for performing the steps of claim 1, when said program is run on a computer" is met on column 6, lines 58-60.

With respect to Claim 13, the limitation of "program code means stored on a computer readable medium for performing the method of claim 1, when said program product is run on a computer" is met on column 6, lines 58-63.

With respect to Claim 14, the limitation of "a computing means" is met by Fig. 2, reference number 50. The CPU represents the computing means. The rest of the limitation has already been discussed in claim 1 rejection.

With respect to Claim 15, the limitation of "computing means" is met by Fig. 2, reference number 50 and "a trusted computing base (TCB) comprising a generator-module for creating a program-specific identifier *(H(D)*" on column 6, lines 34-38; and "a sender-module for sending from said message-originator program (D) a message comprising said program-specific identifier *(H(D))*, said program-specific identifier *(H(D))* being verifiable at said message-receiver program (S) whether it is known to said message-receiver program (S)" is met on column 6, lines

64-67 and on column 7, lines 1-2. The web browser installed certificates are inherently done so by a trusted source.

Claims 5, 6, 7, 8, 9 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Curtis (6023764) in view of Chan et al (6748538 B1).

With respect to Claim 5, Curtis meets all the limitation except the following limitation. The limitation of "wherein a substantially unique cryptographic identifier that is derived by applying a cryptographic function (H) to the message-originator program (D), preferably a hash function, and more preferably a one-way-hash function, such as MD5 or SHA-1, is used as the program-specific identifier (H(D))" is met by Chan et al on column 3, lines 20-30 and lines 49-61.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Chan et al within the system of Curtis because a hash function is a well known protocol that provides a secure way of transmitting a value from a sender to a receiver. This is because a hash function is computationally difficult to reverse and hence this prevents the message from being deciphered by an attacker.

With respect to Claim 6, Curtis meets all the limitation except for the following limitation. The limitation of "the step of signing the program-specific identifier (H(D)) and/or the message by use of a private cryptographic key (k^{-1}) to establish trust between different programs" is met by Chan on column 3, lines 61-63.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Chan within the system of Curtis because digitally signing a message is a well known method of authenticating the sender of the message.

With respect to Claim 7, Curtis meets all the limitation except for the following limitation. The limitation of "wherein the message further comprises an additional program-specific identifier (H((G)) that is signed by use of the private cryptographic key (k-') to establish a membership of an additional program in a trust relationship" is met by Chan et al on column 3, lines 61-63.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Chan within the system of Curtis because digitally signing a message is a well known method of authenticating the sender of the message.

With respect to Claim 8, Curtis meets all the limitation except for the following limitation. The limitation of "wherein the message-receiver program (S) has a public cryptographic key (k)" is met by Chan et al on column 4, lines 33-36.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Chan within the system of Curtis because digitally signing a message is a well known method of authenticating the sender of the message.

With respect to Claim 9, Curtis meets all the limitation except for the following limitation. The limitation of "wherein the message-receiver program (S) and/or the trusted

computing base (TCB) uses a list comprising pre-stored program-specific identifiers and wherein said message-receiver program (S) verifies whether the program-specific identifier *(H(D))* is identical to one of said pre-stored program-specific identifiers" is met by Chan et al on column 4, lines 20-30.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Chan within the system of Curtis because a hash function is a well known protocol that provides a secure way of transmitting a value from a sender to a receiver. This is because a hash function is computationally difficult to reverse and hence this prevents the message from being deciphered by an attacker.

With respect to Claim 10, Curtis meets all the limitation except for the following limitation. The limitation of "wherein the message-receiver program (S) sends a rejection-message if the program-specific identifier (H(D)) is not verified as being known" is met by Chan et al on column 4, lines 23-27.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Chan within the system of Curtis because a hash function is a well known protocol that provides a secure way of transmitting a value from a sender to a receiver. This is because a hash function is computationally difficult to reverse and hence this prevents the message from being deciphered by an attacker.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tracey Akpati whose telephone number is 703-305-7820. The examiner can normally be reached on 8.30am-6.00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Please note the Patent Office will be moving to the Alexandria campus next month. The new phone number for myself, Tracey Akpati is (571) 272-3846, my SPE, Kim Vu is (571) 272-3859 and the receptionist is (571) 272-2100.

AU 2135

OTA